Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277

JOINT COMMENTS OF
MICROSOFT CORPORATION, SKYPE INC. AND YAHOO! INC.

Kevin Minsky
Policy Counsel, U.S. - Legal - Corporate Affairs
MICROSOFT CORPORATION
One Microsoft Way, Bldg. 8
Redmond, WA 98052
425-704-8437
kminsky@microsoft.com

Christopher Libertelli
Director, Government & Regulatory Affairs | N.A.
SKYPE INC.
2145 Hamilton Avenue
San Jose, CA 95125
Skype In: +1202.470.3230
christopher.libertelli@skype.net

James W. Hedlund
Director, Communications Policy
YAHOO! INC.
444 North Capitol Street, N.W., Suite 605
Washington, DC 20001
202-777-1049
hedlund@yahoo-inc.com

A. Richard Metzger, Jr.
Ruth Milkman
A. Renee Callahan
LAWLER, METZGER, MILKMAN & KEENEY, LLC
2001 K Street, NW, Suite 802
Washington, DC 20006
202-777-7700
rcallahan@lmmk.com

Counsel for Microsoft Corporation, Skype Inc. and Yahoo! Inc.

April 28, 2006

Table of Contents

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277

JOINT COMMENTS OF
MICROSOFT CORPORATION, SKYPE INC., AND YAHOO! INC.

Microsoft Corporation ("Microsoft"), Skype Inc. ("Skype") and Yahoo! Inc. ("Yahoo!") (collectively, the "Internet Companies") submit these joint comments in response to the Notice of Proposed Rulemaking ("NPRM") adopted by the Federal Communications Commission ("FCC" or "Commission") in the above-captioned proceeding.[1]

I. INTRODUCTION AND SUMMARY

Microsoft, Skype, and Yahoo! fully support the Commission's efforts to ensure that adequate safeguards are in place to protect against the unauthorized disclosure of Consumer Proprietary Network Information ("CPNI"). Although none of the three firms is a telecommunications carrier and, consequently, none is subject to the provisions of section 222 of

---

[1] *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information*, Notice of Proposed Rulemaking, 21 FCC Rcd 1782 (2006) (FCC 06-10) ("NPRM").

the Communications Act of 1934, as amended ("Act"),[2] all three are subject to federal privacy restrictions and are firmly committed to protecting the privacy of their customers. Indeed, each firm has developed and implemented comprehensive privacy policies that safeguard sensitive billing and other personal information the firms obtain in the course of furnishing their software applications and other products to their customers. Imposing additional new record-keeping or other obligations on the Internet Companies and similarly situated firms would needlessly raise the cost of providing the innovative applications and other products that Microsoft, Skype, and Yahoo! offer, while doing little to enhance consumer privacy. Moreover, the Commission's authority to impose privacy obligations on non-carriers under Title I of the Act is strictly limited. In short, the Internet Companies submit that an effort by the Commission to extend EPIC's proposed privacy obligations to non-carriers would be both unwise as a policy matter and impermissible under the Commission's existing authority.

II. DISCUSSION

A. The Internet Companies Provide Instant Messaging-Based Applications that Allow Members to Make PC-to-PC, One-Way PC-to-PSTN, and/or One-Way PSTN-to-PC VoIP Calls.

Section 222 and the FCC's NPRM focus on protecting sensitive personal data that telecommunications carriers obtain in the course of providing traditional, two-way switched voice telephone service. None of the voice over Internet protocol ("VoIP") offerings of the Internet Companies, however, is comparable to traditional, two-way switched voice service. Rather, the Internet Companies offer consumers the ability to download to their personal computers ("PCs") software applications that enable a number of instant messaging-based functions, including the ability to make VoIP calls. As discussed below, each company currently

---

[2] 47 U.S.C. § 222.

offers a free PC-to-PC VoIP application, as well as one or more separate products that permit users to place one-way (inbound-only or outbound-only) VoIP calls to the Public Switched Telephone Network ("PSTN"). Each of these products incorporates a number of enhanced computer capabilities that distinguish it from traditional switched voice telephony and enable users to customize their online VoIP experiences through various interactive features.[3]

1. *Microsoft*

Microsoft provides computer and software applications, products, and technologies for consumers and businesses. Microsoft's instant messaging application, MSN Messenger, enables users to engage in free PC-to-PC audio calls, video conversations, instant messaging, and/or text messaging to mobile phones.[4] By registering with MSN Messenger and downloading the Messenger software, users are able to set up a list of "contacts" (other Messenger users) with whom they regularly communicate. When a user signs on to Messenger, the user can see whether his or her "contacts" are online and available to chat/talk. MSN Messenger requires users to provide their own Internet access (*e.g.*, DSL, cable, or wireless access). For PC-to-PC VoIP calls, such communications are peer-to-peer between the users' computers, and Microsoft provides no transmission capacity. MSN Messenger also contains a variety of other innovative,

---

[3] The Commission previously has held that certain types of VoIP services are information services, subject to the agency's Title I jurisdiction. *See Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service*, Memorandum Opinion and Order, 19 FCC Rcd 3307, ¶¶ 11-14 (2004) ("*Pulver Order*"). The Internet Companies also offer a vast array of other non-VoIP software applications and other products that are clearly not information services and, therefore, not implicated in this proceeding. The privacy policies that the Internet Companies have implemented with respect to those products, however, are subject to the jurisdiction of the Federal Trade Commission.

[4] *See* Microsoft Online Services: MSN Messenger, *available at*: <http://join.msn.com/messenger/overview/>.

interactive features, including the ability to send files and photos, play games, share musical tastes, and conduct shared Internet searches among two users simultaneously in real-time.

Microsoft is also *beta* testing Windows Live Messenger, the next-generation MSN Messenger application. In addition to offering all the innovative and interactive capabilities of MSN Messenger, Windows Live Messenger allows members to access a "Web Calling" feature that is offered by MCI/Verizon and enables members to make one-way outbound PC-to-PSTN calls.[5] Members obtain the offering directly from MCI/Verizon, which handles all aspects of the PC-to-PSTN offering, including customer registration, account management, customer support, and charging and collecting fees for the service. The transmission/termination of these PC-to-PSTN calls occurs on the MCI/Verizon network. Windows Live Messenger also provides other enhanced capabilities, such as its "Video Conversation" feature, which enables users to engage in video calls with other Windows Live Messenger users that have full-screen (640 x 480 pixels) video and fully synchronized audio.

2. *Skype*[6]

Skype develops Internet communications software applications and offers free PC-to-PC VoIP software to consumers worldwide.[7] By registering with Skype and downloading its software, users are able to make free voice or video calls, or send instant messages ("IM") to other Skype users. The Skype software maintains a distributed directory of Skype users so that users wishing to communicate with other Skype users can announce their online availability.

---

5 *See* "Microsoft and MCI Join to Deliver Consumer PC-to-Phone Calling," *available at*: <http://www.microsoft.com/presspass/press/2005/dec05/12-12MCIPCToPhonePR.mspx> (Dec. 12, 2005).

6 eBay Inc., which runs an online marketplace, is the parent company of Skype and PayPal, but both of the latter companies retain separate corporate identities.

7 *See* Skype Home Page, *available at*: <http://www.skype.com/helloagain.html>.

Skype requires users to provide their own Internet connections, and works in conjunction with the end user's existing broadband Internet access (*e.g.*, DSL, cable modem, wireless). Because Skype routes communications in a peer-to-peer fashion, it utilizes strong encryption to ensure that no peer or other unauthorized party may intercept a communication before it arrives at its intended destination.

Skype also markets two separate product offerings, known as Skype Out and Skype In, to consumers for a fee. Skype Out allows users to complete one-way PC-to-PSTN calls using one of Skype's third-party providers. No numbering resources are used (*i.e.*, no telephone number is assigned to the call), and Skype users who purchase only Skype Out cannot receive calls from the PSTN. Skype also offers a *beta* version of a separate product, Skype In, which allows users to receive calls from the PSTN. Through this offering, one of Skype's provider partners assigns phone numbers to the Skype In subscribers and delivers to those subscribers incoming calls from the PSTN. Skype Out and Skype In are completely separate and independent one-way offerings, with separate pricing schedules, and relatively few users purchase both offerings.

3. *Yahoo!*

Yahoo! provides a variety of online products and services for consumers and businesses to connect with Internet users around the world.[8] Yahoo!'s instant messaging application, Yahoo! Messenger with Voice, allows consumers to make PC-to-PC calls to other Messenger users anywhere in the world for free.[9] By downloading Yahoo! Messenger's software and registering with Yahoo!, users are able to set up a list of contacts. If a contact is available online,

---

[8] Yahoo! Inc. is filing these comments on behalf of itself and its subsidiaries including Yahoo! Communications USA Inc., which provides PC-to-PSTN and PSTN-to-PC services to U.S. subscribers.

[9] *See* Yahoo! Messenger with Voice Home Page, *available at*: <http://messenger.yahoo.com/>.

users can begin a text, voice, or video conversation with the click of a button. If a contact is not available, users may send a text message or leave a voicemail that can be retrieved easily. Yahoo! Messenger with Voice enables users to share photos, play games, or search the Internet, and is integrated with other Yahoo! applications, including Yahoo! 360, which allows members to receive instant notification when new content (such as a blog entry, bookmark or photo) is posted, and Yahoo! Music Unlimited, Yahoo!'s music subscription service. Yahoo! Messenger with Voice requires end users to provide their own Internet connections.

Yahoo! recently introduced in the United States a new version of its instant messaging application, Yahoo! Messenger with Voice, which offers members enhanced PC-based calling capabilities. In addition to the features offered by the original Messenger with Voice, the new version offers separate "Phone Out" and "Phone In" products for a fee. Phone Out enables U.S. members to make outgoing PC-to-PSTN phone calls to traditional and mobile phones. Yahoo! relies on third-party provider partners to terminate Phone Out calls to the PSTN. Phone In allows U.S. users to receive calls on their PCs from traditional and mobile phones. Phone In users are able to select personal phone numbers[10] and receive incoming calls from the PSTN. Phone In and Phone Out are completely separate and independent offerings, with separate pricing schedules. There is no requirement on users to purchase either or both applications. Users can and do purchase only Phone Out without purchasing Phone In and *vice versa*.[11] Because these applications serve different purposes for different users, Yahoo! offers them on an unbundled basis.

---

[10] Yahoo!'s Phone Out service provides users with telephone numbers that Yahoo! obtains from its third-party provider partners.

[11] On April 26, 2006, Yahoo! and AT&T announced the release of a co-branded version of Yahoo! Messenger with Voice to AT&T Yahoo! High Speed Internet subscribers and all Yahoo! users in AT&T's traditional 13-state local service area.

B. New Regulatory Requirements Are Unnecessary Because the Internet Companies Have Implemented Comprehensive Safeguards to Protect the Privacy of Sensitive Customer Information and Are Already Subject to Federal Privacy Restrictions.

Microsoft, Skype, and Yahoo! take seriously the task of protecting their users' privacy. Accordingly, each company has endeavored to use its expertise with respect to cutting-edge Internet technologies to afford its users comprehensive privacy protections that apply across the full range of the company's Internet Protocol ("IP")-enabled products. The Internet Companies have memorialized these protections in privacy policies that strictly guard against unauthorized disclosure of sensitive consumer information. These policies are described in detail on the Internet Companies' web sites and are available to users 24 hours a day, 365 days a year.[12] In addition to such internal protections, the Internet Companies are already subject to federal statutes that protect the privacy rights of consumers, including Section 5 of the Federal Trade Commission Act ("FTC Act").[13] Given the existing statutory regime and the companies' current privacy policies, imposing new CPNI-like regulatory requirements on the Internet Companies would not be justified.

---

[12] *See* Microsoft's policies at: <http://privacy.microsoft.com/en-us/default.aspx>; Skype's policies at: <http://www.skype.com/company/legal/privacy/privacy_general.html>; and Yahoo!'s policies at: <http://privacy.yahoo.com/privacy/us/mesg/index.html>.

[13] 15 U.S.C. § 45. Another federal privacy statute that applies to the Internet Companies is the Electronic Communications Privacy Act. *See* 18 U.S.C. §§ 2510, 2701-2712 (addressing privacy rights for customers and subscribers of computer network service providers).

1. *Privacy Policies*

The Internet Companies have already implemented comprehensive safeguards to protect the privacy of sensitive customer information. The key elements of those safeguards are summarized below for each company.[14]

Microsoft. Microsoft is a certified licensee of TRUSTe,[15] a non-profit entity founded by the Electronic Frontier Foundation and the CommerceNet Consortium to act as an independent, unbiased trust entity for Internet privacy.[16] As a TRUSTe licensee member, Microsoft's privacy and information policies have been reviewed by TRUSTe for compliance. TRUSTe compliance programs address several areas,[17] including:

- General Web Privacy Program Requirements;[18]
- European Union Safe Harbor Privacy Program Requirements;[19]

---

[14] In addition to the safeguards summarized below, each company has other policies designed to protect consumer information (*e.g.*, information provided by children) that is beyond the scope of the NPRM.

[15] *See* TRUSTe seal holder list, *available at*: <http://www.truste.org/about/member_list.php#M>.

[16] *See* TRUSTe Mission Statement, *available at*: <http://www.truste.org/about/mission_statement.php.> TRUSTe's mission is to build trust and confidence in the Internet by promoting the use of fair information practices. TRUSTe monitors its members' privacy policies and practices, certifies that those policies and practices comply with one of several TRUSTe programs, awards each certified company an appropriate "seal" (*e.g.*, the EU Safe Harbor Seal), and helps resolve consumer complaints regarding a certified company's privacy practices.

[17] *See* TRUSTe Program Requirements, *available at*: <http://www.truste.org/requirements.php#req1>.

[18] These requirements include: user controls for e-mail subscriptions; user consent for sharing of personally-identifiable information with third parties; security measures for collecting sensitive information, such as use of secure socket layer protocol; a complaint resolution process, including resolution through TRUSTe for disputes; and disclosure of privacy policies to users. *Id.*

[19] Under the Safe Harbor guidelines, companies must self-certify their compliance with a number of privacy requirements regarding the collection, use, and retention of personal data

- Children's Privacy Seal Program Requirements;
- E-Health Privacy Seal Program Requirements; and
- Email Privacy Seal Program Requirements.

Microsoft's privacy policy, which is available at *http://privacy.microsoft.com/en-us/default.aspx*, provides its end users additional privacy protections, including the following:

- In order to access Microsoft applications (including MSN Messenger) that require users to provide personal information, the user is asked to sign in with an e-mail address and password ("credentials") via secure socket layer ("SSL") protocol. A unique ID number is assigned to the credentials to enhance security.[20]
- Microsoft does not sell, rent, or lease its customer lists to unaffiliated third parties.
- Microsoft does not share its users' personal information with unaffiliated third parties without the user's consent, except as required by law or in limited circumstances – *e.g.*, (1) in response to a court order; (2) in urgent circumstances to protect the personal safety of users of Microsoft applications or members of the public; or (3) occasionally to other companies that provide services on Microsoft's behalf. However, these companies are permitted to obtain only the personal information they need to deliver the service, are required to maintain the confidentiality of the information, and are prohibited from using the information for any other purpose.
- Users may view or edit their personal information online. In order to help prevent a user's personal information from being viewed by others, the user is required to sign in with his or her credentials. The sign-in process is protected by the SSL protocol.
- Microsoft uses a variety of security technologies and procedures to help protect its users' personal information from unauthorized access, use, or disclosure. For example, where users' personal information is stored, it is on computer systems that have limited access and that are located in controlled facilities. When Microsoft

---

from the EU. *See* U.S. Department of Commerce, "Introduction to the Safe Harbor" and associated links, *available at*: <http://www.export.gov/safeharbor/>.

[20] Users of Windows Live Messenger's PC-to-PSTN calling feature are directed to create an account with MCI/Verizon, which maintains its own privacy policy. *See also* Messenger Privacy Supplement, *available at*: <http://privacy.microsoft.com/en-us/messenger.aspx>. Microsoft does not share any of its users' personally identifiable information with MCI/Verizon. Furthermore, Microsoft does not receive any users' MCI/Verizon account information. Microsoft only receives an MCI/Verizon confirmation that a user's account has been created and the user's available minutes so that his or her balance can be displayed in Windows Live Messenger.

transmits highly confidential information (such as a credit card number or password) over the Internet, it protects such information through the use of encryption, such as the SSL protocol.

Skype. From its inception in 2002, Skype has consciously integrated privacy protections into all levels of its applications and into the very architecture of its system. Skype privacy practices are in accordance with applicable data protection regulations, including the EU data protection and information security requirements, which are among the highest standards in the world. Skype's privacy policy, which is available at *http://www.skype.com/company/legal/privacy/privacy_general.html*,[21] provides its users a range of protections, including the following:

- Prior to using Skype, individuals are required to register by providing a "Skype name" and password.

- Skype does not sell, rent, trade or otherwise transfer any personal information or communications content to any third party without the user's explicit permission, except as required by law or in certain limited circumstances. For example, Skype may occasionally share personal data with its affiliates, partner service providers, or agents. Skype always requires these third parties to take appropriate organizational and technical measures to protect any personal and traffic data they receive, and to observe any relevant statute.

- Skype does not retain its users' personal and traffic data any longer than needed to bill the user, as required by law, to ensure the proper functioning of its software, or for the purposes specifically permitted by its privacy policy.

- Through a password-protected website, Skype enables users to access a very limited amount of information, primarily for customer use in connection with the SkypeOut product. For each call, this information is limited to the date the call was placed, the called number, the country of destination, the rate for the call, and the duration and price of the call.

- Skype takes appropriate organizational and technical measures to protect the personal and traffic data collected by it. For example, a user's personal and traffic data can be accessed only by authorized employees of Skype who need to have access to these data in order to fulfill their given duties. To the extent information, such as call detail

---

[21] *See also* Skype Privacy FAQ, *available at*: <http://www.skype.com/help/faq/privacy.html>.

or other sensitive information is captured in connection with Skype's paid applications, that information also is protected by multiple layers of security.

- Skype also takes appropriate technical measures to protect the confidentiality of the communications content of its users' calls. For example, calls between Skype users are encrypted end-to-end via 256-bit Advanced Encryption Standard, also known as Rijndael.

- A Skype user can view, correct, complete, or remove personal data maintained by Skype, but only after Skype verifies the identity of the user.

Yahoo! Yahoo! is certified by TRUSTe as a holder of its Web Privacy Seal,[22] which identifies companies that adhere to TRUSTe's strict privacy principles and comply with the TRUSTe dispute resolution process.[23] Yahoo!'s privacy policy, which is available at *http://privacy.yahoo.com/privacy/us/mesg/index.html*,[24] provides its end users various privacy protections, including the following:

- Prior to using Yahoo! Messenger with Voice, a person must register with Yahoo! by providing certain personal information. The user also is required to create a password to prevent unauthorized access to the account and to safeguard the information contained in it.

- Yahoo! does not rent, sell, or share personal information about its users with unaffiliated third parties without the user's permission, except as required by law or under certain limited circumstances that are fully disclosed in Yahoo!'s privacy policy. For example, Yahoo! provides personal information to trusted partners who work on behalf of or with Yahoo! under confidentiality agreements.

- Any user may edit his or her Yahoo! Account Information, including marketing preferences, at any time, by logging into his or her account and providing a password that is verified by Yahoo!.

---

22 *See* TRUSTe seal holder list, *available at*: <http://www.truste.org/about/member_list.php#Y>.

23 For more information about the Web Privacy Seal, *see* "TRUSTe Marks Trustworthy Companies," *available at*: <http://www.truste.org/about/web_privacy_seal.php>; *see also supra* pages 8-9 & nn.14-17.

24 *See also* Privacy Practices for Yahoo! Messenger with Voice, *available at*: <http://privacy.yahoo.com/privacy/us/mesg/details.html>.

- Yahoo! limits access to its users' personal information to employees who reasonably need to come into contact with that information to provide products or applications to the user or to do their jobs.

- Yahoo! has implemented physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about its users. For example, Yahoo! uses SSL encryption when transmitting certain kinds of information, such as financial services information or payment information.

As the foregoing summaries make clear, the Internet Companies already have implemented a robust suite of privacy safeguards, including some of the safeguards proposed by EPIC (*e.g.*, consumer-set passwords). It would be unnecessary and unreasonably burdensome for the FCC to impose additional requirements on these VoIP providers, particularly since the FTC already has ample authority to police their privacy practices for any unfair or deceptive acts.

2. *Existing Federal Privacy Regulation*

There is no need for the Commission to subject VoIP providers to another privacy regime that was designed to protect CPNI collected by *telecommunications carriers*, which are not subject to the FTC's jurisdiction.[25] Doing so would needlessly burden VoIP providers (contrary to Congress's stated intent),[26] while doing little to enhance consumer privacy.

Section 5 of the FTC Act declares "unfair or deceptive acts or practices" in or affecting commerce to be illegal,[27] and confers on the FTC the plenary power to prevent such acts and

---

25 15 U.S.C. § 45(a)(2). Because telecommunications carriers are not subject to the FTC's jurisdiction, their privacy practices are, by necessity, overseen primarily by the FCC pursuant to section 222 of the Act, while the privacy practices of information service providers and other firms are regulated by the FTC. *See* Letter from Deborah Platt Majoras, Chairman, FTC, to Hon. F. James Sensenbrenner, Jr., Chairman, Committee on the Judiciary, U.S. House of Representatives, at 3 (April 14, 2006) ("The FTC is the only federal agency with general jurisdiction over consumer protection and competition in most sectors of the economy, including broadband Internet access services.").

26 *See* discussion *infra* Section II.D.

27 15 U.S.C. § 45(a)(1).

practices.[28] Accordingly, the FTC may, upon conducting a formal hearing, issue a "cease and desist order" to stop the unfair or deceptive act.[29] Anyone who does not comply with an FTC order is subject to a civil penalty of up to $11,000, with each day of a continuing violation constituting a separate violation.[30]

In recent years, the FTC has brought a number of cases against companies, including information service providers, that allegedly deceived the public by violating the terms of their own privacy policies.[31] In 2000, for example, a bankrupt website agreed to settle charges it violated Section 5 by representing to consumers that personal information would never be shared with third parties and then disclosing, selling or offering that information for sale.[32] Earlier this year, a consumer data broker agreed to settle charges that it had disclosed consumers' sensitive personal information to subscribers in a manner that was not consistent with the broker's publicized privacy principles, despite the fact that the subscribers' applications to the broker raised obvious "red flags" about the legitimacy of their data requests.[33]

Even if a company has not deceived the public by violating its own privacy policy, it may be subject to FTC charges that the company's treatment of sensitive customer information is "unfair" under Section 5. For example, an Internet company that provides shopping cart software

---

28 15 U.S.C. § 45(a)(2).

29 15 U.S.C. § 45(b).

30 15 U.S.C. § 45(l); 16 C.F.R. § 1.98.

31 *See* FTC, "Enforcing Privacy Promises: Section 5 of the FTC Act," *available at*: <http://www.ftc.gov/privacy/privacyinitiatives/promises.html>.

32 *See* FTC Press Release, *available at*: <http://www.ftc.gov/opa/2000/07/toysmart2.htm> ("ToySmart Press Release").

33 The data broker also allegedly violated the Fair Credit Reporting Act. *See* FTC Press Release, *available at*: <http://www.ftc.gov/opa/2006/01/choicepoint.htm> ("ChoicePoint Press Release").

to online merchants recently agreed to settle charges that it unfairly rented personal information about merchants' customers to marketers, knowing that such disclosure contradicted merchant privacy policies.[34] Likewise, a discount shoe retailer recently agreed to settle FTC charges that its failure to take reasonable security measures to protect sensitive customer data against hackers was an unfair practice that violated Section 5.[35]

In these and other recent Section 5 cases, the FTC has secured settlements that impose very substantial assessments and/or require companies to submit to FTC oversight for a lengthy period (*e.g.*, 20 years). Under one court-ordered settlement, for instance, the allegedly malfeasant company was required to pay $10 million in civil penalties – the largest civil penalty in FTC history – and $5 million in consumer redress for violating the Fair Credit Reporting Act and Section 5 of the FTC Act.[36] Other remedies imposed in recent settlements include the following: requiring companies to implement a comprehensive information security program that includes administrative, technical, and physical safeguards;[37] requiring companies to obtain

---

34 *See* FTC Press Release, *available at*: <http://www.ftc.gov/opa/2005/03/cartmanager.htm> ("CartManager Press Release").

35 *See* FTC Press Release, *available at*: <http://www.ftc.gov/opa/2005/12/dsw.htm> ("DSW Press Release"). The FTC has obtained consent agreements from a number of other companies that it pursued for alleged failures to take reasonable security measures to protect sensitive data, claiming that such failures amount to an unfair trade practice in violation of Section 5. *See, e.g.*, FTC Press Release, *available at*: <http://www.ftc.gov/opa/2005/06/bjswholesale.htm> ("BJs Press Release"); FTC Press Release, *available at*: <http://www.ftc.gov/opa/2006/02/cardsystems_r.htm> ("CardSystems Press Release").

36 *See* ChoicePoint Press Release; *United States v. ChoicePoint Inc.*, "Stipulated Final Judgment and Order" at 4, 17, *available at*: <http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf>. The FTC has obtained injunctive and other equitable relief, including monetary relief for consumer redress or disgorgement of ill-gotten profits, pursuant to section 13(b) of the FTC Act. 15 U.S.C. § 53(b).

37 *See* ChoicePoint Press Release; DSW Press Release; BJs Press Release; CardSystems Press Release.

audits from an independent, third-party security professional every other year for 20 years;[38] subjecting companies to record-keeping and reporting provisions to allow the FTC to monitor compliance;[39] and requiring companies to disgorge fees made through the allegedly unfair renting of consumers' personal information.[40]

As the FTC's aggressive enforcement of Section 5 makes clear, VoIP providers are already subject to effective federal oversight designed to protect the privacy of consumer information. The broad scope of these precedents suggests, moreover, that the FTC has ample authority under Section 5 to address the types of abuses described in the NPRM, including a failure by VoIP providers adequately to protect customer information from unauthorized disclosure to data brokers.[41] There is simply no need for the FCC to burden VoIP providers with a new layer of privacy regulations that, at best, would duplicate existing internal and statutory protections, or, at worst, would conflict with those existing safeguards.

C. The VoIP Offerings by Microsoft, Skype, and Yahoo! Are Not Telecommunications Services, and, Therefore, Are Not Subject to Section 222 of the Act.

The Internet Companies' privacy safeguards described above are largely the result of the proactive commitment by each of the companies to develop and implement a comprehensive plan

---

38 *See ChoicePoint Press Release; DSW Press Release; BJs Press Release; CardSystems Press Release.*

39 *See* ChoicePoint Press Release; CartManager Press Release; DSW Press Release.

40 *See* CartManager Press Release.

41 In recent Congressional testimony, the FTC affirmed that it is strongly committed to investigating companies that engage in pretexting and that it will not hesitate to prosecute "[c]ompanies that have failed to implement reasonable security and safeguard processes for consumer data." Prepared Statement, at 8, of Lydia B. Parnes, Director, Bureau of Consumer Protection, Federal Trade Commission, "Protecting Consumers' Phone Records," Senate Committee on Commerce, Science, and Transportation: Subcommittee on Consumer Affairs, Product Safety, and Insurance (Feb. 8, 2006), *available at*: <http://commerce.senate.gov/pdf/parnes-020806.pdf>.

for protecting personal customer information required to provide each company's various applications and products, and not an FCC mandate. As explained above, these policies already fall under FTC oversight. Furthermore, as explained below, the VoIP applications offered by Microsoft, Skype, and Yahoo!, including PC-to-PC and one-way PC-to-PSTN and PSTN-to-PC VoIP, are information services and, consequently, are not subject to the requirements of section 222 that apply to telecommunications services.[42]

The VoIP offerings of the Internet Companies provide consumers "a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications."[43] Specifically, the Internet Companies make available to users integrated software applications/interfaces that perform enhanced computer processing functions, including, for example, storing and retrieving users' contact lists, acquiring and retrieving information about users' online availability, and making available certain information necessary to authenticate end-user members. The Internet Companies' one-way PC-to-PSTN and PSTN-to-PC VoIP applications also transform end-user information from one protocol to another, *i.e.*, from IP to circuit-switched/PSTN signaling protocols, or *vice versa*. As the FCC has recognized, "an end-to-end protocol conversion service that enables an end-user to send information into a network in one protocol and have it exit the network in a different protocol

---

42 The FCC has held repeatedly that information services are not Title II services. *See, e.g.*, 47 C.F.R. § 64.702(a); *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd 14853, ¶ 108 (2005) ("Title II obligations have never generally applied to information services, including Internet access services.") (citing precedents). As noted above, non-VoIP software applications and other products offered by the Internet Companies are not within the Commission's jurisdiction because they are neither telecommunications nor information services. The Internet Companies' privacy policies applicable to those products would be subject to the jurisdiction of the Federal Trade Commission, as are the privacy policies of most commercial firms.

43 *See* 47 U.S.C. § 153(20) (defining information services).

clearly 'transforms' user information," thus rendering it an information service under the Act.[44] Each of the functionalities described above offers the Internet Companies' users enhanced processing abilities that are the hallmark of an information service. Moreover, because PC-to-PC VoIP and many (if not all) configurations of the one-way VoIP applications provided by the Internet Companies require users to supply their own transmission, these applications do not constitute "telecommunications," and thus are not "telecommunications services."[45] Accordingly, the Internet Companies' VoIP products are information services that are not subject to Title II of the Act.[46]

D. Courts Have Strictly Limited the Commission's Authority Under Title I of the Act to Impose Title II Obligations on Non-Carriers.

Even assuming, *arguendo*, that the Commission were to consider imposing new privacy obligations on information service providers, its authority to do so under Title I of the Act is

---

44 *See Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, First Report and Order and Further Notice of Proposed Rulemaking, 11 FCC Rcd 21905, ¶¶ 104-106 (1997).

45 *See Pulver Order* ¶¶ 9-10. The FCC further recognized in the *Pulver Order* that certain information transmitted by VoIP applications (*e.g.*, a user's online availability) is new information that is not "telecommunications," as defined in the statute, because it is not information "of the user's choosing, without change in the form or content . . . as sent and received." *Id.* ¶ 9. The Internet Companies' VoIP applications provide similar information about a user's online availability.

46 *Federal-State Joint Board on Universal Service*, Report to Congress, 13 FCC Rcd 11501, ¶ 39 (1998) ("[W]hen an entity offers transmission incorporating the 'capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information,' it does not offer telecommunications. Rather, it offers an 'information service' even though it uses telecommunications to do so."). Because VoIP applications are information services, the Commission also should clarify that state commissions are preempted from imposing additional privacy obligations on IP-enabled service providers. *See Vonage Holdings Corporation Petition for Declaratory Ruling Concerning an Order of the Minnesota Public Utilities Commission*, Memorandum Opinion and Order, 19 FCC Rcd 22404, ¶ 1 (2004) (preempting state regulation of VoIP applications), *appeal pending, Minnesota Pub. Utils. Comm'n v. FCC*, No. 05-1069 (8th Cir., filed Jan. 6, 2005).

doubtful. Title I confers limited *ancillary* authority on the Commission that the agency may exercise only if two conditions are met: (i) the subject of the proposed regulation is covered by the FCC's general grant of jurisdiction under Title I of the Act, which encompasses "all interstate and foreign communication by wire or radio;"[47] and (ii) the subject of the regulation is "reasonably ancillary" to the FCC's effective performance of its statutorily mandated responsibilities.[48] An attempt to impose new privacy obligations, such as those proposed by EPIC, on the Internet Companies' VoIP applications would not withstand scrutiny under these standards.

As an initial matter, the Commission lacks subject matter jurisdiction under Title I to regulate a VoIP provider's post-transmission practices regarding sensitive customer information. Certain of the potential new obligations that have been suggested – *e.g.*, deleting or encrypting stored sensitive customer data, maintaining "audit trails" regarding the disclosure of such data, and post-transmission breach notice requirements – would appear to seek to regulate practices that occur entirely after a VoIP call has terminated.[49] The recent decision of the D.C. Circuit in the "Broadcast Flag" case makes clear that, while the FCC may properly assert its ancillary

---

47 47 U.S.C. §§ 151, 152(a).

48 *United States v. Southwestern Cable Co.*, 392 U.S. 157, 178 (1968) ("*Southwestern Cable*"); *American Library Ass'n v. FCC*, 406 F.3d 689, 700 (D.C. Cir. 2005) ("*American Library*"). To be sure, if both conditions are satisfied, the FCC "has jurisdiction to impose additional regulatory obligations [on information service providers] under its Title I ancillary jurisdiction to regulate interstate and foreign communications." *National Cable & Telecommunications Ass'n v. Brand X Internet Servs.*, __ U.S. __, 125 S. Ct. 2688, 2696 (2005); *see also id.* at 2708. Nothing in this terse observation purports to modify or otherwise call into question the Supreme Court's long-standing insistence that the assertion of ancillary jurisdiction is proper only where the FCC both has general subject matter jurisdiction and the proposed regulation is "reasonably ancillary" to the FCC's effective performance of its statutory duties.

49 NPRM ¶¶ 17, 19, 20.

jurisdiction to regulate activity involving the "process of radio or wire transmission,"[50] its jurisdiction does not extend to practices occurring "only *after*" a transmission is complete.[51]

Moreover, extending the proposed regulations to non-carriers would not be "reasonably ancillary" to the FCC's effective performance of its statutory duties. As the Supreme Court has established, such regulations may be adopted only when they are both "necessary to ensure the achievement of the Commission's statutory responsibilities"[52] and consistent with the Act's other provisions.[53] When one or both of these requirements is lacking, courts have not hesitated to strike down regulations premised on the FCC's Title I authority – particularly where such regulations would effectively convert non-carriers to "common-carrier status."

For example, in *Midwest Video*, the Supreme Court held the FCC lacked ancillary authority to adopt regulations that would have "[e]ffectively . . . relegated cable systems, *pro tanto*, to common-carrier status."[54] The Court rejected the FCC's argument that the proposed rules would serve a statutory purpose, finding instead that they were inconsistent with the express directive of the Act that the FCC not treat persons engaged in broadcasting as common carriers.[55]

---

50 *American Library*, 406 F.3d at 700, 703, 705, 706, 707, 708.

51 *Id.* at 691 (FCC lacks authority to impose regulation whose effect occurs entirely "*after* a broadcast transmission is complete") (emphasis in original).

52 *FCC v. Midwest Video Corp.*, 440 U.S. 689, 706 (1979) ("*Midwest Video*"); *see also Pulver Order* ¶ 19 n.69 ("Congress has provided the Commission with ancillary authority under Title I to impose such regulations as may be necessary to carry out its other mandates under the Act."); *IP-Enabled Services*, Notice of Proposed Rulemaking, 19 FCC Rcd 4863 ¶ 46 (2004) ("*IP-Enabled NPRM*") ("Title I of the Act confers upon the Commission ancillary jurisdiction over matters that are not expressly within the scope of a specific statutory mandate but nevertheless necessary to the Commission's execution of its statutorily prescribed functions.").

53 *See, e.g.*, *Midwest Video*, 440 U.S. at 702-708; *Pulver Order* ¶ 19 n.69.

54 *Midwest Video*, 440 U.S. at 700-701.

55 *Id.* at 702.

In the instant proceeding, extending the proposed privacy regulations to non-carriers would not be "necessary" for the FCC to carry out its mandate under any Title II section, including section 222. In order to satisfy that requirement, the FCC must establish a direct nexus between the Title I communication it seeks to regulate and the protection or promotion of a specific non-Title I responsibility set forth in the Act. For example, in *Southwestern Cable*, the Court upheld the Commission's determination that the achievement of various broadcast-related purposes under Title III of the Act (*e.g.*, the orderly development of a national system of local broadcast systems) was placed in jeopardy by the "explosive growth" of cable television, and therefore required regulation of cable pursuant to the FCC's ancillary jurisdiction.[56] Other courts and the FCC itself have insisted that such a nexus be established as a prerequisite to the proper assertion of ancillary jurisdiction.[57]

In the instant case, the FCC's imposition of new privacy requirements on VoIP providers would not enhance the FCC's ability to carry out a specific statutory duty under Title II of the

---

56 *Southwestern Cable*, 392 U.S. at 174-77.

57 *See, e.g.*, *Computer and Communications Industry Ass'n v. FCC*, 693 F.2d 198, 213 (D.C. Cir. 1982) (FCC's exertion of ancillary jurisdiction over enhanced services and customer premises equipment was "reasonably ancillary" under *Southwestern Cable* because it was necessary to assure that Title II communications services were offered at reasonable rates), *cert. denied sub nom. Louisiana PSC v. FCC*, 461 U.S. 938 (1983); *Motion Picture Ass'n of America v. FCC*, 309 F.3d 796, 804-806 (D.C. Cir. 2002) (Congress's delegation of authority to FCC under section 1 of the Act was not, by itself, a sufficient basis for FCC to require "video descriptions" for television programming pursuant to its ancillary jurisdiction); *Implementation of Sections 255 and 251(a)(2) of the Communications Act of 1934, as Enacted by the Telecommunications Act of 1996*, Report and Order and Further Notice of Inquiry, 16 FCC Rcd 6417, ¶ 99 (1999) (assertion of ancillary jurisdiction to ensure the accessibility of two information services – voicemail and interactive menu service – to persons with disabilities is proper because both services are "so integral to the use of telecommunications services today that, if inaccessible and unusable, the underlying telecommunications services that sections 255 and 251(a)(2) have sought to make available will not be accessible to persons with disabilities in a meaningful way. In short, inaccessible voicemail and interactive menus could defeat the effective implementation of sections 255 and 251(a)(2).").

Act. For example, extending the requirements to VoIP providers would not safeguard the FCC's ability to achieve the stated purpose of the NPRM: "to further protect the privacy of customer proprietary network information (CPNI) that is collected and held *by telecommunications carriers*" in accord with section 222.[58] As noted, moreover, the Internet Companies have already instituted stringent privacy policies to protect sensitive billing and other information about their customers. Further, as discussed above, information pertaining to VoIP customers is already protected by federal statutes (including the FTC Act), and VoIP providers have devoted considerable resources to ensure compliance with those regimes. Subjecting those providers to a new, largely duplicative and potentially inconsistent layer of CPNI regulations would be a wholly *unnecessary* step that cannot be justified by the FCC's ancillary jurisdiction under Title I.

Extending section 222 and other proposed regulations to non-carriers also would be inconsistent with the Commission's "decades old goals and objectives to enable information services to function in a freely competitive, unregulated environment."[59] In addition, such an initiative would directly contravene Congress's express statutory directives that CPNI obligations be limited to "telecommunications carrier[s]"[60] and that the "Internet and other interactive computer services [remain] unfettered by Federal or State regulation."[61] Based on those considerations, the FCC in 2004 "expressly decline[d]" to exercise Title I jurisdiction to

---

58 NPRM ¶ 1 (emphasis added).

59 *Pulver Order* ¶ 19 n.69. While the FCC in this proceeding and in the *IP-Enabled Services* proceeding sought comment on the appropriate scope of social policy obligations for IP services, it also reaffirmed its commitment to preserving a "'hands-off' approach," under which IP-enabled services are only "minimally regulated." *IP-Enabled NPRM* ¶¶ 5, 39; *see also id.*, ¶ 39 (noting "Congress's clear intention, as expressed in the 1996 Act, that such services remain 'unfettered' by federal or state regulation") (citing 47 U.S.C. §§ 230(b), 157 & nt.).

60 47 U.S.C. § 222.

61 47 U.S.C. § 230(b)(2); *see also* Section 706 of the Act, 47 U.S.C. § 157 nt.

impose Title II-type economic and entry/exit regulations on a VoIP application offered by pulver.com.[62] The Commission should exercise the same prudent restraint in the instant proceeding.

In sum, there is no sound legal or factual basis for the Commission to seek to regulate the privacy practices of non-carrier VoIP providers pursuant to its ancillary jurisdiction under Title I of the Act. If the Commission nonetheless were to ignore this record and seek to exercise its ancillary authority to extend section 222 or other privacy obligations to VoIP applications, it should limit that extension to those VoIP products that consumers reasonably expect to function as replacements for "regular telephone" service, as it has done in the past.[63] Specifically, in the *VoIP E911 Order* adopted last year, the Commission asserted its Title I jurisdiction to regulate only those VoIP products "that enable[] a customer to do everything (or nearly everything) the customer could do using an analog telephone."[64] Based on this standard, the Commission imposed new E911 regulations only on real-time, two-way interconnected VoIP providers that enable consumers to both make calls to and receive calls from the PSTN.[65] Any new regulations adopted in the instant proceeding should, at most, apply only to the same subset of VoIP offerings.[66]

---

62 *Pulver Order* ¶ 19 n.69.

63 *IP-Enabled Services, E911 Requirements for IP-Enabled Service Providers*, First Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd 10245, ¶ 23 (2005) ("*VoIP E911 Order*").

64 *Id.*; *see also id.* ¶¶ 26-35 (discussing authority to impose E911 regulations under Title I).

65 *Id.* ¶ 24.

66 Under no circumstances should the Commission attempt to extend any new rules to apply to private IP-enabled networks operated by end-user customers. Even where the FCC clearly possesses Title II jurisdiction over carriers, it has not attempted to subject end-user customers of those carriers to carrier regulation. *A fortiori*, the FCC should not seek to assert jurisdiction over end-user customers that operate private IP-enabled networks. *See id.* ¶ 24 n.78 (declining to

III. CONCLUSION

For the foregoing reasons, Microsoft, Skype, and Yahoo! urge the Commission not to impose CPNI privacy regulations on non-carrier providers of VoIP applications.

Respectfully submitted,

/s/ A. Richard Metzger, Jr.
A. Richard Metzger, Jr.
Ruth Milkman
A. Renee Callahan
LAWLER, METZGER, MILKMAN & KEENEY, LLC
2001 K Street, NW, Suite 802
Washington, DC 20006
202-777-7700
rcallahan@lmmk.com

Counsel for Microsoft Corporation, Skype Inc. and Yahoo! Inc.

Kevin Minsky
Policy Counsel, U.S. - Legal - Corporate Affairs
MICROSOFT CORPORATION
One Microsoft Way, Bldg. 8
Redmond, WA 98052
425-704-8437
kminsky@microsoft.com

Christopher Libertelli
Director, Government & Regulatory Affairs | N.A.
SKYPE INC.
2145 Hamilton Avenue
San Jose, CA 95125
Skype In: +1202.470.3230
christopher.libertelli@skype.net

James W. Hedlund
Director, Communications Policy
YAHOO! INC.
444 North Capitol Street, N.W., Suite 605
Washington, DC 20001
202-777-1049
hedlund@yahoo-inc.com

April 28, 2006

---

extend new rules to end-user customers' use of IP-compatible customer equipment, such as an IP-PBX, to create their own private IP networks).

Certificate of Service

I, Ruth E. Holder, hereby certify that on this 28th day of April, 2006, I caused true and correct copies of the foregoing Joint Comments of Microsoft Corporation, Skype Inc. and Yahoo! Inc. to be mailed by electronic mail to:

Janice Myles
Competition Policy Division
Wireline Competition Bureau
Federal Communications Commission
janice.myles@fcc.gov

and

Best Copy and Printing, Inc.
fcc@bcpiweb.com

/s/ Ruth E. Holder
Ruth E. Holder